Deepali A. Brahmbhatt (SBN 255646)
Email: dbrahmbhatt@devlinlawfirm.com
Hayden B. Corrales (SBN 350580)
Email: hcorrales@devlinlawfirm.com
DEVLIN LAW FIRM LLC
3120 Scott Blvd. #13,
Santa Clara, CA 95054
Telephone: (650) 254-9805

Timothy Devlin (*pro hac vice* pending)
Email: tdevlin@devlinlawfirm.com
Devlin Law Firm LLC
1526 Gilpin Avenue
Wilmington, DE 19806
Telephone: (302) 449-9010

Attorneys for Plaintiffs and the Class
Dr. Monica Mehring and Dr. Monica Mehring Family Dentistry on behalf of herself, her business and all others similarly situated

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

Dr. Monica Mehring and Monica Mehring, DDS, LLC doing business as Dr. Monica Mehring Family Dentistry, on behalf of herself, her business and all others similarly situated,

Plaintiffs,

vs.

PATTERSON COMPANIES INC. *dba* PATTERSON DENTAL,
CHANGE HEALTHCARE,
OPTUM, INC., and
UNITEDHEALTH GROUP INC.,
Defendants.

Case No. **4:24-cv-3147**

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Monica Mehring and her business Mehring Family Dentistry ("Plaintiffs") bring this Class Action Complaint against Defendants Patterson Companies Inc. doing business as Patterson Dental, and against UnitedHealth Group and its subsidiaries Change Healthcare and Optum Inc. (collectively, "UHG"), by and through its attorneys in their individual capacity and on behalf of others similarly situated. Plaintiffs assert the following allegations based on their personal knowledge of their own actions, as well as investigations conducted by their counsel, and upon information and belief regarding all other relevant matters:

I. NATURE OF ACTION

1. Plaintiffs brings this proposed class action lawsuit against Defendants Patterson Dental, Change Healthcare Inc., Optum, Inc. and UnitedHealth Group Incorporated ("Defendants") for their failure to maintain the security of their computer networks in accordance with state and federal law. Defendants' computer networks include data processing systems, portals, and platforms that have become critical infrastructure for administering healthcare across the United States. Defendants' computer networks process billions of healthcare transactions annually for more than one million healthcare providers of all kinds. Defendants have broadened the reach of their services via acquisition to include various systems that healthcare providers use to submit claims for payment verify individuals' insurance coverage and authorizations, and many other critical functions.

2. Given their role in the nationwide delivery of healthcare, Defendants knew (or should have known) they needed to implement robust cybersecurity controls to prevent disruptions. Defendants failed in this obligation. As a result of Defendants' negligence, failures, and omissions, a group of cybercriminals was able to infiltrate Defendants' computers networks and steal for ransom confidential health data and source code, among other things ("Data

Breach"). The group of cybercriminals may be ALPHV/Blackcat group ("Blackcat") or the RansomHub gang.

3. As a result of the Data Breach, which exposed the vulnerabilities in Defendants' computer networks, Defendants took all of the affected computer networks offline. From the time the Data Breach was discovered on February 21, 2024 and in many aspects ongoing through date of filing of this Complaint, healthcare providers were unable to provide critical services and get paid on claims. Defendants' negligence, failures, and omissions have harmed hard-working medical providers around the country, including Plaintiffs.

4. Given the amount of confidential personal health information ("PHI") and personal identifying information ("PII") that healthcare organizations maintain, government agencies have warned for years about the threat of cyberattacks. The U.S. government has also warned the industry that Blackhat has hit at least 70 organizations since December 2023, a majority of them healthcare organizations. Therefore, the Data Breach and related shutdown were entirely foreseeable and could have—and should have—been avoided.

5. Plaintiffs, individually and on behalf of all others similarly situated, alleges claims for negligence, negligent interference with prospective economic advantage, breach of express and/or implied contractual promise, breach of covenant of good faith and fair dealing and for unjust enrichment.

II. PARTIES

6. Plaintiff Dr. Monica Mehring is a licensed dentist and operates her business Monica Mehring, DDS, LLC doing business as Dr. Monica Mehring Family Dentistry in the state of Delaware.

7. On information and belief, Defendant Patterson Companies Inc. dba Patterson Dental is a Minnesota Corporation that has branches throughout the United States including in this District at 5087 Commercial Circle Suite 20, CONCORD, CA 94520. Patterson Dental's Eaglesoft software using Change Healthcare and Optum software to integrate processing prescriptions, billing and insurance.

8. On information and belief, Defendant Change Healthcare Inc. is a publicly traded company with its principal place of business in Nashville, Tennessee and is incorporated in Delaware. On information and belief, it became a subsidiary of UnitedHealth Group Incorporated in 2022 and is operated by Optum, Inc., another UnitedHealth Group subsidiary. Change Healthcare, Inc. ("Change Healthcare") is among the largest prescription medication processors in the United States.

9. On information and belief, Defendant UnitedHealth Group Incorporated is one of the largest publicly traded companies by revenue. It is incorporated in Delaware and maintains its principal place of business in Minnetonka, Minnesota. UnitedHealth Group exercises control over the management of the Change Healthcare cybersecurity systems as evidenced by UnitedHealth Group's response to the Data Breach as alleged herein.

10. On information and belief, Defendant Optum, Inc. maintains its principal place of business in Eden Prairie, Minnesota and is incorporated in Delaware. UnitedHealth Group Incorporated, a massive healthcare conglomerate, includes Optum, Inc. divisions: Optum Health, OptumInsight, and Optum Rx (collectively, "Optum"). (Ex. A, Q.).

11. According to Optum, in October 2022, UnitedHealth Group incorporated finalized its acquisition of Change Healthcare and integrated it with OptumInsight "to provide software and data analytics, technology-enabled services and research, advisory and revenue cycle management offerings to help make health care work better for everyone." (*See* Ex. B, M, O, P.)

III. JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are more than one hundred members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interests and costs, and this is a class action in which one or more members of the proposed Class, including Plaintiffs, are citizens of a state different from Defendants. The Court

has supplemental jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the same case or controversy.

13. This Court has personal jurisdiction over Defendants. Defendant Patterson Dental has branches in this State and routinely conducts business in the State within this District. All Defendants are registered to conduct business in California; have sufficient minimum contacts in California; and intentionally avail themselves of the markets within California through the promotion, sale, and marketing of their services, thus rendering the exercise of jurisdiction by this Court proper and necessary.

14. Venue is proper in this District under 28 U.S.C. § 1391 because Plaintiffs' injuries arise from use of Patterson Dental's Eaglesoft software that Defendant provides nationwide including in this District. Defendant Change Healthcare, Optum and United HealthGroup's integration of Eaglesoft is also provided nationwide including in this District.

IV. REQUIREMENTS FOR SECURING PERSONAL IDENTIFYING INFORMATION AND SENSITIVE HEALTH RELATED INFORMATION

15. Defendants' software systems did not meet industry security standards including those established by Federal and state regulators. Industry standards are established to govern the creation, collection, protecting, and use of private information including sensitive health information. There are well-established guidelines and recommendations to reduce the risk of cyberattacks, data breaches, and the resulting harm to consumers and the healthcare industry. Compliance with industry security standards is required by numerous state and federal laws.

16. Defendants' software was not in compliance with these industry standards and several state and federal laws. Defendants were or should have been fully aware of their duty to secure such sensitive health information.

17. Change is a HIPAA-covered entity. Change states in its Global Privacy Notice that it "functions as a HIPAA business associate for its HIPAA covered entity payer and provider customers as its primary business function, so Change Healthcare's creation, collection, use, and

disclosure of protected health information is guided by HIPAA and the terms of a business associate agreement and other contracts." (Ex. C.)

18. Defendants are required to comply with HIPAA Rules, including the Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. HIPAA's Standards for Privacy of Individually Identifiable Health Information (also known as the "Privacy Rule") establishes national standards for the protection of medical records and other personal health information. HIPAA's Security Standards for the Protection of Electronic Protected Health Information (also known as the "Security Rule") establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. Per the U.S. Department of Health and Human Services' website, "[t]he Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information." (*See* Ex. D.)

V. FEBRUARY 2024 DATA BREACH

19. On February 21, 2024, Defendants discovered the Data Breach and that their computer networks were not secure and could not protect PHI and PII as required by state and federal law. UHG set up a website regarding the Data Breach at www.unitedhealthgroup.com to announce the Data Breach and stated that it disconnected the Change Healthcare systems. UHG made a similar statement in a filing with the U.S. Securities and Exchange Commission. UHG also stated, "The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies . . . At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational." (*See* Ex. D-E.)

20. UHG admits that its systems and services became non-operational. For example, UHG said in a statement: "We are working aggressively on the restoration of our systems and

services." UHG also stated, "All of us at UnitedHealth Group feel a deep sense of responsibility for recovery and are working tirelessly to ensure that providers can care for their patients and run their practices, and that patients can get their medications. We're determined to make this right as fast as possible." (*See* Ex. F.)

21. UnitedHealth Group paid a $22 million ransom to hackers. (*See* Ex. G.)

22. Sen. Thom Tillis, R-N.C., held up a bright yellow copy of "Hacking for Dummies" during the hearing, saying the breach is UnitedHealth's responsibility to fix. "This is some basic stuff that was missed, so shame on internal audit, external audit and your systems folks tasked with redundancy, they're not doing their job," Tillis said. (*Id.*)

23. A second group is demanding ransom, stating that UnitedHealth Group paid its original ransom to the wrong hackers. (Ex. H.)

24. The Data Breach was foreseeable, Defendants were on notice, and reasonable precautions could have prevented it.

25. The Healthcare industry is more attractive to cybercriminals because of the sensitive nature of the confidential health and personal information maintained and stored by healthcare organizations. Ransomware attacks in the healthcare industry are on the rise, doubling in the past five years as reported by FBI. (*See* Ex. I-J).

26. Gaining access to even encrypted health data is considered disclosure. A ransomware fact sheet disclosed by the Department of Health and Human Services makes it clear that for entities covered by HIPAA, "When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (*i.e.*, unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule." (Ex. K.)

27. Under the HIPAA Privacy Rules, a breach is defined as, "[t]he acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." The Data Breach qualifies as a breach under

the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule.

28. A ransomware attack is also considered a "Security Incident" under HIPAA. Under the HIPAA Rules, a "Security Incident" is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 CFR § 164.304. Here, the Data Breach meets the Security Incident definition of the HIPAA Rules. (*See* Ex. K.)

29. The UHG family had experienced a previous recent data breach, demonstrating alack of reasonable diligence in complying with the security standards. (*See* Ex. L, UHG press notification regarding credential stuffing attack in May of 2023.)

30. Defendants knew that Plaintiffs and Class members depended on Defendants (either directly or via agents) to acquire and transmit PHI and PII securely, and also store and maintain such information securely. Defendants should also know that they were a likely target for cybercriminals given the rise of such incidents in the healthcare industry and their own recent experience. Defendants failed to take reasonable measures to avoid cyberattacks. Defendants' non-compliance with reasonable and lawful security standards, and failure to take reasonable measures to avoid cyberattacks, resulted in the Data Breach, shutdown and harm to Plaintiffs and Class members.

31. Defendants' positioned themselves as dependable healthcare provider that would handle PHI and PII appropriately. Defendants did the opposite, making the data vulnerable to attacks. Defendants failed to comply with applicable laws to properly secure their computer networks and maintain PHI and PII. On information and belief, Defendants did not upgrade their technology to utilize the latest in security technology to prevent attacks and the Data Breach.

32. Plaintiffs and the members of the Class entrusted Defendants (or their partners who Defendants entrusted in turn) with PHI and PII. Defendants had the resources necessary to prevent the Data Breach and to protect their computer networks, but neglected to adequately

invest in security measures despite their obligations to do so. Accordingly, Defendants breached their common law, statutory and other duties owed to Plaintiffs and Class members.

33. Defendants' duty to use reasonable security measures also arose under HIPAA. UHG is covered by HIPAA and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. Under HIPAA, Defendants were required to "reasonably protect" PHI from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

34. Under HIPAA, Defendants were specifically required to do the following: (1) ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted. 45 C.F.R. § 164.306(a)(1); (2) implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1); (3) implement adequate policies and procedures to prevent detect, contain, and correct security violations. 45 C.F.R. § 164.308(a)(1)(i); (4) implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports. 45 C.F.R. § 164.308(a)(1)(ii)(D); (5) protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI. 45 C.F.R. § 164.306(a)(2); (6) protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information. 45 C.F.R. § 164.306(a)(3); (7) ensure compliance with HIPAA security standard rules by its workforces. 45 C.F.R. § 164.306(a)(4); (8) train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI. 45 C.F.R. § 164.530(b); and/or (9)

render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304 definition of encryption).

35. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendants.

36. The Data Breach and resulting shutdown of the Change Healthcare networks were a direct and proximate result of Defendants' failure to: (1) properly safeguard and protect computer networks with PHI and PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (2) establish and implement appropriate safeguards to ensure the security and confidentiality of PHI and PII; and (3) protect against reasonably foreseeable threats to the security or integrity of such information and computer networks.

VI. PLAINTIFFS' HARM

37. Plaintiffs Dr. Monica Mehring and her business Dr. Monica Mehring Family Dentistry are licensed healthcare providers serving patients in Newark, Delaware.

38. Plaintiffs contract with Patterson Dental for its Eaglesoft software for integrated practice management including tools to streamline their operations.

39. Eaglesoft in turn, is integrated with Change Healthcare and Optum to process insurance claims submitted by its clients, among other things.

40. Beginning on or around February 21, 2024, when Defendants' systems were shut down as a result of the Data Breach, Plaintiffs could no longer submit claims through Eaglesoft and obtain payments for those claims. Moreover, Plaintiffs have been unable to receive payments for claims submitted on February 20, 2024. Since the shutdown, Plaintiffs payments were

interrupted for any claims despite continuing to treat patients. Plaintiffs rely on the payments they receive from submitted claims to pay basic business expenses, including salaries and wages to employees, and to further grow the practice. As a workaround, Plaintiffs have switched to a different software for insurance claims payments. Electronic billing is still not working. Software for prescriptions is also interrupted and not fixed.

41. Plaintiff had to take credit from her home equity line of credit to pay bills and minimize impact on payroll for her employees caused by the Data Breach.

42. Plaintiffs and the Class have suffered severe and lasting consequences because of the Data Breach. (*See* Ex. N.)

43. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiffs staff resources have been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

VII. CLASS ACTION ALLEGATIONS

44. Plaintiffs bring this action individually and on behalf of all other persons similarly situated (the "Nationwide Class") pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4).

45. The Nationwide Class is defined as follows:

> All healthcare providers in the United States whose use of Change Healthcare's and Optum's services were disrupted by the data breach occurring in February 2024.

46. Additionally, pursuant to the Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs bring this action on behalf of the following Delaware Class defined as:

> All healthcare providers in the state of Delaware whose use of Change Healthcare's and Optum's services were disrupted by the data breach occurring in February 2024.

47. The Nationwide Class specific to Patterson Dental is defined as follows:

All healthcare providers in the United States whose use of Patterson Dental's Eaglesoft's services were disrupted by the data breach occurring in February 2024.

48. Additionally, pursuant to the Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs bring this action on behalf of the following Delaware Patterson Dental Class defined as:

All healthcare providers in the state of Delaware whose use of Patterson Dental's services were disrupted by the data breach occurring in February 2024.

49. The Nationwide Class and the Delaware Class are collectively referred to herein as the "Class," unless otherwise stated.

50. Excluded from the proposed Class are Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

51. Plaintiffs reserve the right to re-define the Class definitions after conducting discovery.

52. **Numerosity (Fed. R. Civ. P. 23(a)(1))**. The Class members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes over one million licensed healthcare providers. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

53. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3))**. Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but are not limited to, the following: (a) whether Defendants breached their legal duty to Plaintiffs and Class members; (b) whether Defendants had a special relationship with Plaintiffs and Class members; (c) whether Defendants are liable for negligence to Plaintiffs and Class members; (d) whether

Defendants negligently interfered with Plaintiffs and Class members' prospective economic advantage; (e) whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendants' conduct; and (f) Whether Plaintiffs and Class members are entitled to relief, including damages and equitable relief.

54. **Typicality (Fed. R. Civ. P. 23(a)(3))**. Pursuant to Rule 23(a)(3), Plaintiff's claims are typical of the claims of the Class members. Plaintiff, like all Class members, suffered harm as a result of the Data Breach and ensuing shutdown of Defendants' computer networks.

55. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4))**. Pursuant to Rule 23(a)(4), Plaintiffs and its counsel will fairly and adequately protect the interests of the Class. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs have retained counsel experienced in prosecuting class actions and data breach cases.

56. **Superiority (Fed. R. Civ. P. 23(b)(3))**. Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class members because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

57. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because: (a) the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual Class members which would establish incompatible standards of conduct for Defendants; or (b) the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to individual Class members which would, as a practical matter, be dispositive of the interests of other Class members not

parties to the adjudications, or substantially impair or impede their ability to protect their interests; or (c) Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

58. **Issue Certification (Fed. R. Civ. P. 23(c)(4))**. In the alternative, the common questions of fact and law, set forth in Paragraphs above, are appropriate for issue certification on behalf of the proposed Class.

VIII. CAUSES OF ACTION

COUNT I: NEGLIGENCE

59. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

60. Defendants had (and continue to have) a legal duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting confidential health and personal identifying information on their network systems. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated.

61. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them and Plaintiffs and Class members, which is recognized by state and federal law, including but not limited to HIPAA. Only Defendants, however, were in a position to ensure that their computer networks were sufficient to protect against the harm to Plaintiffs and the Class members that resulted from the Data Breach and ensuing shutdown.

62. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting PHI and PII on their network systems by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PHI and PII entrusted to them. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting PHI and PII by

failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in harm to Plaintiffs and Class members.

63. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiffs and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting their data networks and PHI and PII within their possession, custody and control, which resulted in the shutdown of Defendants' computer networks and disrupted Plaintiffs and Class members' businesses.

64. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiffs and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting PHI and PII.

65. But for Defendants' negligent breach of the above-described duties owed to Plaintiffs and Class members, Defendants would not have experienced the Data Breach and would not have had to shut down the Change Healthcare networks, thereby preventing Plaintiffs and Class members from (i) timely receiving payments for previously submitted claims, (ii) submitting new claims for payment, and (iii) obtaining insurance authorization for patient medical treatment, among other things. The harm to Plaintiffs and Class members were foreseeable given the types of services Defendants provide and the statutory obligations shared by all to protective computer networks and confidential PHI and PII.

66. Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and resulted in the shutdown of the Change Healthcare and Optum computer networks constitute negligence. Defendants are jointly and severally liable for these actions or omissions causing the Data Breach.

67. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and the related shutdown, Plaintiffs and Class members have suffered (and will continue to suffer) monetary losses and economic harms and seek all available damages.

COUNT II: NEGLIGENT INTERFERENCE WITH PROSPECTIVE ECONOMIC ADVANTAGE

68. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

69. Plaintiffs had an ongoing business relationship with Patterson Dental with use of Eaglesoft that would have likely resulted in future economic benefits to Plaintiffs.

70. Defendants knew or should have known about Plaintiff's relationship with Patterson Dental due to the integration of Change Healthcare's and Optum's services and processes with Eaglesoft.

71. The harm to Plaintiffs resulting from the Data Breach and shutdown was foreseeable.

72. Defendants failed to act with reasonable care and engaged in wrongful conduct, including by violating the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et. seq.*), and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801).

73. Plaintiffs' use of Eaglesoft has been disrupted, resulting in economic harm to Plaintiff.

74. Defendants' wrongful conduct was a substantial factor in causing the harm to Plaintiffs and Class members. Plaintiffs and Class members seek all available damages. Defendants are jointly and severally liable for these actions or omissions causing the Data Breach.

COUNT III: NEGLIGENCE PER SE

75. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

76. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . [p]ractices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect PHI. Various FTC publications and orders also form the basis of Defendants' duty.

77. Defendants violated Section 5 of the FTC Act (and analogous state laws) by neglecting to implement reasonable measures to safeguard PHI and by failing to adhere to industry standards. Defendants' actions were notably unreasonable, considering the type and volume of PHI acquired and stored, as well as the foreseeable ramifications of a data breach on Defendants' systems.

78. UHG falls under the purview of HIPAA, per 45 C.F.R. § 160.102, and thus is mandated to adhere to all rules and regulations outlined in 45 C.F.R. Parts 160 and 164.

79. "Security and Privacy" are governed by 45 C.F.R. Part 164, where Subpart A offers "General Provisions," Subpart B regulates "Security Standards for the Protection of Electronic Protected Health Information," Subpart C outlines requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governs the "Privacy of Individually Identifiable Health Information."

80. According to 45 C.F.R. § 164.104, the "standards, requirements, and implementation specifications adopted under this part" are applicable to covered entities and their business associates, including UHG.

81. UHG is required by HIPAA to guarantee the "confidentiality, integrity, and availability of all electronic protected health information" it handles and to safeguard against anticipated threats or hazards to the security or integrity of such information, as outlined in 45 C.F.R. § 164.306.

82. UHG breached HIPAA regulations by failing to comply with and meet the mandated standards delineated in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

83. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

84. Defendants violated HIPAA (and analogous state statutes) by neglecting to employ reasonable measures to safeguard PHI and by failing to adhere to industry standards.

85. Defendants' violation of Section 5 of the FTC Act and HIPAA (and similar state statutes) constitutes negligence *per se.*

86. Class members are individuals falling within the category of persons intended to be protected by Section 5 of the FTC Act and HIPAA (along with comparable state statutes).

87. Further, the harm involved in this Data Breach aligns with the type of harm intended to be prevented by the FTC Act and HIPAA (as well as comparable state statutes). In fact, the FTC has initiated over fifty enforcement actions against businesses that, due to their failure to implement reasonable data security measures and refrain from engaging in unfair and deceptive practices, caused harm similar to that experienced by Plaintiffs and Class Members.

88. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PHI of Plaintiffs and the Class would not have been compromised.

89. There is a close causal connection between Defendants' failure to implement security measures to protect the PHI of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PHI of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

90. As a direct and proximate result of Defendants' negligence per se, Plaintiffs and the Class have incurred and will continue to endure various forms of harm, including but not

limited to: (i) invasion of privacy; (ii) theft of their PHI; (iii) depreciation or loss of value of PHI; (iv) expended time and opportunity costs associated with mitigating the actual repercussions of the Data Breach; (v) deprivation of the expected benefits from the agreement; (vi) missed opportunities and costs incurred while trying to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the persistent and heightened risk to their PHI, which: (a) remains unencrypted and vulnerable to unauthorized access and misuse by third parties; and (b) continues to be backed up in Defendants' possession, subjecting it to further unauthorized disclosures as long as Defendants neglects to implement appropriate and sufficient protective measures for the PHI.

91. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

92. Additionally, as a direct and proximate result of Defendants' negligence per se, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI in its continued possession. Defendants are jointly and severally liable for these actions or omissions causing the Data Breach.

93. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

94. Defendants' negligent conduct is ongoing, in that it still holds the PHI of Plaintiffs and Class Members in an unsafe and insecure manner.

COUNT IV: BREACH OF IMPLIED CONTRACT

95. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs above.

96. Plaintiffs and Class Members were required to provide their PHI to Defendants as a condition of receiving services from Defendants and/or its clients.

97. Plaintiffs and the Class entrusted their PHI to Defendants. In so doing, Plaintiffs and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

98. Implicit in the agreement between Plaintiffs, Class Members, and the Defendants regarding the provision of PHI, which Plaintiffs and Class Members were required to provide to Defendants, were the following obligations for the Defendants: (a) restrict the use of such PHI solely for business purposes, (b) implement reasonable measures to safeguard the PHI, (c) prevent unauthorized disclosures of the PHI, (d) promptly and adequately notify Plaintiffs and Class Members of any unauthorized access and/or theft of their PHI, (e) reasonably safeguard and protect the PHI of Plaintiffs and Class Members from unauthorized disclosure or use, and (f) maintain the PHI under conditions ensuring its security and confidentiality.

99. The mutual understanding and intent between Plaintiffs, Class Members, and Defendants are evident through their conduct and ongoing business interactions.

100. Defendants solicited, offered, and invited Plaintiffs and Class Members to provide their PHI as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their PHI to Defendants.

101. In accepting the PHI of Plaintiffs and Class Members, Defendants understood and agreed that it was required to reasonably safeguard the PHI from unauthorized access or disclosure.

102. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiffs and Class Members that they would only disclose PHI under certain circumstances, none of which relate to the Data Breach.

103. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PHI would remain protected.

104. When entering into these implied contracts, Plaintiffs and Class Members reasonably believed and anticipated that Defendants' data security practices adhered to pertinent laws and regulations and aligned with industry standards.

105. Plaintiffs paid money to Patterson Dental for its services, which benefited all Defendants. Plaintiffs and Class members had a reasonable belief and expectation that Defendants would maintain adequate data security. Defendant failed to do so. Plaintiffs and the Class have paid money directly or indirectly to UHG.

106. Plaintiffs and Class Members would not have entrusted their PHI to Defendants in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

107. Plaintiffs and Class Members would not have entrusted their PHI to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

108. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

109. Defendants breached the implied contracts they made with Plaintiffs and the Class by failing to safeguard and protect personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach

110. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain. Defendants are jointly and severally liable for these actions or omissions causing the Data Breach.

111. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT V: BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING

112. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

113. Applicable law implies a covenant of good faith and fair dealing in every contract.

114. Plaintiffs and Class Members are the third-party beneficiaries of contracts between insurers, Patterson Dental and UHG.

115. Plaintiffs performed all of their duties under their agreements with Defendants.

116. All of the conditions required for Defendants' performance under the contracts have occurred.

117. Incorporated in the contracts as a matter of law is the covenant of good faith and fair dealing, which prevents a contracting party from engaging in conduct that frustrates the other party's rights to the benefits of the agreement. The implied covenant imposes on a contracting party not only the duty to refrain from acting in a manner that frustrates performance of the contract, but also the duty to do everything that the contract presupposes that the contracting party will do to accomplish its purposes.

118. Here, the implied covenant of good faith and fair dealing required Defendants, under the terms of their agreement which stated that Defendants would protect PII and PHI, to safeguard and protect from disclosure to third parties the PII and PHI provided by Plaintiffs and the Class Members, which was turned over to Defendants only for the purposes of performing or procuring professional services. Plaintiffs and the Class Members could not enjoy Defendants' services without the safeguarding and protection of the PII and PHI.

119. Defendants breached the covenant of good faith and fair dealing implied in their contracts by engaging in the following conscious and deliberate acts: (a) failing to implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure; and (b) failing to ensure that unauthorized parties were not provided access to Plaintiffs' and Class Members' PII. Defendants' failure to protect the PII of Plaintiffs and Class Members frustrated Plaintiffs' and

Class Members' rights to the benefit of their insurers' bargains with Defendants, to enjoy the professional services of Defendants without incurring risks of property and identity theft.

120. Plaintiffs and Class Members have lost the benefit of their medical providers' and/or insurers' contracts by having their PII compromised and have been placed at an imminent, immediate and continuing risk of identity theft-related harm. Defendants are jointly and severally liable for these actions or omissions causing the Data Breach.

121. As a direct and proximate result of Defendants' breach of the covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial, but in excess of the minimum jurisdictional requirement of this Court.

COUNT VI: UNJUST ENRICHMENT

122. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

123. Plaintiffs and Class members conferred benefits on Defendants in the form of payments for claims management and processing, insurance verification, authorization and medical necessity reviews, and disbursement of payments, among other things, directly and/or indirectly. Defendants had knowledge of the benefits conferred by Plaintiffs and Class members and appreciated such benefits. Defendants should have used, in part, the monies Plaintiffs and Class members paid to it, directly and indirectly, to pay the costs of reasonable data privacy and security practices and procedures. Defendants are jointly and severally liable for these actions or omissions causing the Data Breach.

124. Plaintiffs and Class members have suffered actual damages and harm because of Defendants' conduct, inactions, and omissions. Defendants should be required to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds received from Plaintiffs and Class members.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the members of the Class defined above, respectfully request that this Court enter:

(a) An order certifying this case as a class action under Federal Rule of Civil Procedure 23, appointing Plaintiffs as the Class representative, and appointing the undersigned as Class counsel;

(b) A judgment awarding Plaintiffs and Class members appropriate monetary relief, including actual damages, equitable relief, restitution, and disgorgement;

(c) An order entering injunctive and declaratory relief as appropriate under applicable law;

(d) An order awarding Plaintiffs and the Class pre-judgment and/or post-judgment interest as prescribed by law;

(e) An order awarding reasonable attorneys' fees and costs as permitted by law; and

(f) Any and all other and further relief as may be just and proper.

Dated: May 23, 2024

DEVLIN LAW FIRM, LLC

By: /s/ Deepali A. Brahmbhatt
Deepali A. Brahmbhatt

Deepali A. Brahmbhatt (SBN 255646)
Email: dbrahmbhatt@devlinlawfirm.com
Hayden B. Corrales (SBN 350580)
Email: hcorrales@devlinlawfirm.com
DEVLIN LAW FIRM LLC
3120 Scott Blvd. #13,
Santa Clara, CA 95054
Telephone: (650) 254-9805

Timothy Devlin (*pro hac vice* pending)
Email: tdevlin@devlinlawfirm.com
Devlin Law Firm LLC
1526 Gilpin Avenue
Wilmington, DE 19806
Telephone: (302) 449-9010

Attorneys for Plaintiffs Dr. Monica Mehring and Dr. Monica Mehring Family Dentistry and on behalf of themselves and all others similarly situated

X. DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial.

Dated: May 23, 2024

DEVLIN LAW FIRM, LLC

By: /s/ Deepali A. Brahmbhatt
Deepali A. Brahmbhatt

Deepali A. Brahmbhatt (SBN 255646)
Email: dbrahmbhatt@devlinlawfirm.com
Hayden B. Corrales (SBN 350580)
Email: hcorrales@devlinlawfirm.com
DEVLIN LAW FIRM LLC
3120 Scott Blvd. #13,
Santa Clara, CA 95054
Telephone: (650) 254-9805

Timothy Devlin (*pro hac vice* pending)
Email: tdevlin@devlinlawfirm.com
Devlin Law Firm LLC
1526 Gilpin Avenue
Wilmington, DE 19806
Telephone: (302) 449-9010

Attorneys for Plaintiffs Dr. Monica Mehring and Dr. Monica Mehring Family Dentistry and on behalf of themselves and all others similarly situated